Doc. Ref. N.º:	192.HS_RNCSIRT
Page number:	13
Date:	14.10.2021

hardsecure

FROM:	Hardsecure, Networks and Information Security Systems
TO:	**Rede Nacional CSIRT**
SUBJECT:	Hardsecure's computer security incident response service in accordance with RFC2350
CLASSIFICATION:	PUBLIC

Index

1. DOCUMENTATION CONTROL

1.1. Version history

Version	Date	Description
1.0	30/11/2020	First version

Version	Implemented	Reviewed	Approved
1.1	12/10/2021	14/10/2021	Hardsecure

1.2. Distribution

Name	Organization concerned
	[#Customer]

1.3. Hardsecure's contact information

Name	Address	Email
	Rua Acácio de Paiva, nº 16 - 1º D 1700-006 Lisboa – Portugal Tel.: +351 218 278 126 Email: geral@hardsecure.com	

1.4. Information about the organization

Name	Address	Email

2. INFORMATION ABOUT THIS DOCUMENT

This document describes Hardsecure's computer security incident response service in accordance with RFC2350.

2.1. Last update date

Version 1.1 published on 10/21/14.

2.2. Distribution lists for notifications

There is no distribution channel to notify changes to this document.

2.3. Access to this document

The updated version of this document is available at

https://www.hardsecure.com/services/servico-de-gestao-de-incidentes-de-seguranca-and-ciberseguranca

2.4. Authenticity of this document

This document is signed with the h-CSIRT Hardsecure key. The PGP key used to sign is available in section 3.7.

3. CONTACT INFORMATION

3.1. Team Name

h-CSIRT Hardsecure – Computer Security Incident Response Team at Hardsecure

3.2. Address

h-CSIRT Hardsecure

Rua Engenheiro Frederico Ulrich nº3210, Maia, Portugal

3.3. Time zone

Portugal/WEST (GMT+0, GMT+1 in daylight savings time)

3.4. Telephone

+351 218 278 126 (Normal hours of operation- 9:00 am to 6:00 pm).

+351 915 613 526 (Emergency contact outside normal operating hours).

3.5. Other telecommunications

Non-existent.

3.6. Email addresses

csirt@hardsecure.com - Email for notification of cybersecurity incidents and other matters related to CSIRT services.

3.7. Public keys and cipher information

PGP Key ID: 711C15DD

PGP Fingerprint: 0173 5C4D EB8D 3989 0545 F6BD B371 7D48 711C 15DD

The PGP key can be retrieved from: https://pgp.mit.edu/

3.8. Team members

Coordination: Rui Almeida

Members: Hugo Moreira, Renato Rodrigues, Pedro Lobo, Vitor Teixeira

3.9. Other information

General information about h-CSIRT Hardsecure can be found at https://hardsecure.com.

3.10. Means of contact for users

h-CSIRT Hardsecure has the means of contact listed in sections 3.4 to 3.6

4. SCRIPT

4.1. Mission

Protecting Information Security at Hardsecure and in the community, also cooperating towards a growing cybersecurity resilience in the geographies where Hardsecure is present, through its role of supporting organizations in the sense of being prepared to face threats at the level of cyber-attacks.

4.2. Served Community

h-CSIRT Hardsecure manages the response to security incidents of the information of employees and customers processed or stored in its IT infrastructure or in external IT systems, through actions developed from IP 87.103.13.203, in this case subject to contractual clauses in force.

4.3. Affiliation

h-CSIRT Hardsecure is part of the Security Operations Center, Hardsecure's organizational unit.

4.4. Authority

The assignments of h-CSIRT Hardsecure are defined by its CISO.

5. POLICIES

5.1. Incident Types and Level of Support

h-CSIRT Hardsecure responds to incidents in the areas of computer security, namely intrusion or attempted intrusion, malicious code, availability, collection of information, information security, fraud, abusive content, and vulnerabilities.

In addition to computer security incidents, h-CSIRT Hardsecure responds and intervenes in the areas of secure authentication, lifecycle management of digital identities, cooperation, interaction, definition and privacy policies and data protection.

5.2. Cooperation, interaction, and privacy policy

h-CSIRT Hardsecure's privacy and data protection policy provides that sensitive information may be passed on to third parties, solely and exclusively in case of need and with the express prior authorization of the individual or entity to whom this information concerns.

5.3. Communication and Authentication

The means of communication provided by h-CSIRT Hardsecure, telephone and non-encrypted email are considered sufficient for the transmission of non-sensitive information. For the transmission of sensitive information, it is mandatory to use PGP cipher.

6. SERVICES

Hardsecure guarantees a capacity to provide services that is adequate to the reality of each institution, with technical and operational resources adequate to the provision of advanced security and cybersecurity services, to guarantee the mitigation/blocking of differentiated and distinct attack vectors.

6.1. Defensive Security

Through the use of technical means that allow the blocking/mitigation of attacks to the IT infrastructure of an organization (NG Firewall, endpoint security, DLP, Identity Management, Proxy/Reverse Proxy, Anti-spam, SIEM, Strong Authentication, Anti-target attack, …).

6.2. Security Audits

ISO27001, ISO27002, ISO22301, ISO27005, ISO27037 and PCI-DSS standards.

6.3. Pentest/Pentest as a Service

Vulnerability Assessment, Incident Injection (exploit DB, Zero-day/Zero-hour).

6.4. Forensic Analysis

Email Crime Investigation, Web Attacks Investigation, Operating System Forensics,Data Acquisition and Duplication, Cloud Forensics, Malware Forensics, Mobile Forensics, Network Forensics, Database Forensics.

6.5. Response to Security Incidents

SOC & SOC as a Service

6.6. Code Safety and Quality Control Tests

Use of OWASP, PTES, OWTF, NIST, ISSAF and OSSTMM frameworks.

6.7. Data Protection

Adoption of mechanisms and policies covering Processes and Procedures, Personal Data, Organization, and the Institution's Information System (coordination between IT Security vs. Legal).

6.8. Consultancy

Planning, Governance, Action Plans, Correction/Mitigation.

6.9. Investigation and development

Malware Investigation, Exploit Development, Cybersecurity Projects.

7. SAFEGUARD OF LIABILITY

Although every precaution is taken in the preparation of the information disclosed either on the Internet portal or through distribution lists, h-CSIRT Hardsecure does not assume any responsibility for errors or omissions, or for damages resulting from the use of this information.